Amendments to the Specification and Abstract

In the Specification:

Before paragraph [0001] please delete the heading "Description".

Before paragraph [0002] please delete the heading "Background Information" and insert in its place the heading --BACKGROUND--.

Please replace paragraph [0003] with the following rewritten paragraph:

[0003] The application Cryptoheaven (see ~~http://www.crytoheaven.com~~ http://www.cryptoheaven.com) is a Java application (applet/Java plug-in). Similarly to MS Explorer, the display is divided, on the left, into a directory tree (incl. the local computer) and a contact list. Settings can be made via the right mouse button/popup. A proprietary protocol via port 82 is used. Data compression is used. Files are signed and encrypted. Files can also be uploaded from the local file system using drag and drop (DnD). The sequence control substantially corresponds to that of MS Explorer. The encryption is done locally on the client computer. Directories can be created, deleted and renamed. Access to directories is enabled for "invited users". The invitation is made via e-mail by users who have subscribed to the system. The invited must give his/her consent. Authentication is via user ID and password. The system is available for the operating systems Windows/Unix and Linux.

Please replace paragraph [0004] with the following rewritten paragraph:

[0004] Another typical application exists in bvPREMIERE, bvPRO, bvPLUS+ and big VAULT Enterprise (see http://www.bigvault.com). The applications are specifically for Windows and allow a drive to be mapped (created) in MS Explorer, which is controlled via the WEB. The transmission protocol for uploading and downloading files is html over an ~~SSl~~ SSL connection. File encryption is done on the server. Access to directories and files is enabled using a visitor password. There is an in-tray for authorized users. It is possible to log in as a user or visitor.

Passwords with a limited validity period are set up in the same manner as has been done, for example, in UNIX for many years.

Before paragraph [0007] please insert the heading
--SUMMARY OF THE INVENTION--.

Please replace paragraph [0007] with the following rewritten paragraph:

[0007] With respect to security and to the storage system, the known applications have the following disadvantages:

- A security model based on user name and password can only implement the states access authorization granted or access authorization revoked. Finer control, for example, using time limits or intervals to be observed for access, is not possible~~, nor is it possible to limit the number of simultaneously accessing users~~.

- The storage model used is characterized as a registry of created folders, in which files are stored regardless of their type, and retrieved again ~~unchanged~~. A freely selected classification ~~by content cannot be controlled by the system itself. It is completely impossible for a folder to become active itself and, for example, to make backup copies of stored files, to time stamp the files, or to delete them after predetermined storage periods~~ or restriction by predefined filed types is not possible.

Please replace paragraph [0008] with the following rewritten paragraph:

[0008] ~~The~~ An object of the present invention is to provide a method for access and data storage in telecommunications networks which overcomes the disadvantages of the known applications and provides ~~significantly~~ increased security.

Please replace paragraph [0010] with the following rewritten paragraph:

[0010] The aim of the data transfer is to store data in memories of servers in order to restore the data to the local computer when needed, to have the data processed on a remote computer, or to make the data available to third parties or to the user himself/herself at a different location for a certain period of time. The conditions under which access is allowed ~~must be~~ is able to be precisely controlled and maintained. The storage of files requires a classification system which should provide clarity for the retrieval of files and optimally support data security.

Please replace paragraph [0011] with the following rewritten paragraph:

[0011] The ~~requirements for~~ present invention provides precise access control and a classification system for the storage of the files featuring high security ~~are optimally met by the data storage system of the present invention~~. The data storage system includes the server and its special program operating in a telecommunications network as well as the local computers integrated over the network. The program on the server uses a storage model in the form of a locker system. The locker system has a virtual character because, depending on the access rights, only the lockers and files the user is authorized to access are displayed to the user. No information is provided to the user when access is denied. Instead, the lockers, sub-locker, and files for which the user is not authorized are not displayed to the user.

After paragraph [0013], please insert the heading --BRIEF DESCRIPTION OF THE DRAWINGS-- and new paragraph [0013.1] as follows:

--[0013.1] Fig. 1 shows the structure of server and client programs according to a method for data storage on a server in a telecommunications network;

Fig. 2 shows the steps for encrypting a file to be stored according to a method for data storage on a server in a telecommunications network; and

Fig. 3 shows a locker system according to method a for data storage on a server in a telecommunications network.--.

Before paragraph [0014], please insert the heading --DETAILED DESCRIPTION--.

Please replace paragraph [0014] with the following rewritten paragraph:

[0014] During registration, the server operator creates a personal area of the ~~DS~~ server for the user, said personal area being called the main folder (1) of the user. Operating systems and databases store data and their management information in different ways. Here, the known model of folders (also: directories) and files is used for purposes of description. A file (containing the data) is ~~always~~ contained in a folder, which is either the so-called root folder, or is itself contained in a folder. Thus, starting from this folder, the root folder is reached via a chain of higher-level folders. The names of the folders in this chain are strung together to form the so-called path of the file. A file is uniquely described by its name and path.

Please replace paragraph [0016] with the following rewritten paragraph:

[0016] Figure 3 illustrates the locker system. The main locker (main folder) contains further lockers which are set up by the operator and distinguished by function. These lockers include, inter alia, personal lockers (2), provisioning lockers (3), receiving lockers (4), and public lockers (5) for the ~~user, and a system locker (6) which can only be accessed by the server~~ users. The locker type is specified in the associated special file.

Please replace paragraph [0018] with the following rewritten paragraph:

[0018] Personal lockers contain only user-stored references to the files of the user; the transferred files themselves are stored by the server in the system folder, or locker, (6), which can only be accessed by the server (Figure 1). Provisioning lockers are used by the user to store therein the references to his/her files for other users. Receiving lockers contain references offered to the user by other users, and public lockers contain references to files offered to all users. The user is able to set up sub-lockers in each locker of any of the types mentioned above, and to store references in these sub-lockers. Said sub-lockers may, in turn, contain other sub-lockers.

Please replace paragraph [0020] with the following rewritten paragraph:

[0020] The structure of the server and client programs is illustrated in Figure 1. The server sends a special program, the so-called client program, to the local computer. It is also possible to install a client program on the local computer and to make the connection from the local computer. The client program connects itself to some of the systems existing on the local computer, for example, a smart card reader, a fingerprint scanner, a face recognition system, a GPS module, or a system configured to determine (or to approximately determine) the geographic location.

Please replace paragraph [0027] with the following rewritten paragraph:

[0027] Storing a file located on the local computer into the personal locker of the user is a multi-step process, which is carried out by the user using a program having one component in the client program and one component on the server. The user interface of the client program allows the user to select the file to be stored by path and name and to specify the destination path in his/her personal locker. The steps for encrypting a file to be stored are illustrated in Figure 2. The server informs the client program of the destination locker requirements to be met by the files to be stored. These requirements include the maximum size, specific format (doc, pdf), or the existence of a signature of the data. If the requirements are met, the client program loads the data contained in the file and generates a random number, the so-called access key (8), with which the data is encrypted using a symmetric encryption method. Subsequently, this access key is encrypted with the public user key to form the encrypted access key (9), and the access key is destroyed. In this manner, it is achieved that the encrypted content of the file can be decrypted only by the user who is able to recover the access key with the aid of his/her secret key.

Please replace paragraph [0029] with the following rewritten paragraph:

[0029] If the user, as the owner of a file, wants to offer this file to another user, he/she acts as an administrator and sets up a user locker (7) for the other user in a provisioning locker, as shown in Figure 3. For this purpose, the server offers the user, via the client program, a user directory

which is in the manner of a telephone book and from which the user selects the desired user as the addressee. The user can also set up a personal locker for a group of users. The server enters this user or these users into the properties file as co-owners of the locker.

Before paragraph [0034] please insert new paragraph [00033.1] as follows:

--[0033.1] From the description, it becomes clear that a user sees a reference in his/her client program only if the reference contains an encrypted access key that is encrypted with the public key of the user. Using his/her secret key and the encrypted access key, the user can restore the access key of the file and decrypt the encrypted data.

File information:	Owner	File name	Creation date	Data type/Path	Signature
Access data:					
Right to "access" co-user 1:	location a ... location z	time a ... time z	authentication a ... authentication z	IP address a ... IP address z	network type a ... network type z
Right to "access" co-user n:					
Upper limits:	individual file size	total file size	number of sub-lockers		
Limitations:	file types	signatures			

Table 1: special folder file

Definition:	system-created file; representative of a file in the system locker	
Data fields:	identifier of the referenced file;	

	encrypted encryption key; type of file; size of file; file creation time; reference creation time; time of last access.	
Security information:	owner; restriction authentication	

Table 2: reference--.

Please delete paragraph [0034].